(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開平7－107082
(43)公開日　平成７年(1995)４月21日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ 9/00				
9/10				
9/12				
			Ｈ０４Ｌ 9/00	Ｚ

審査請求　未請求　請求項の数１　ＯＬ　（全 13 頁）

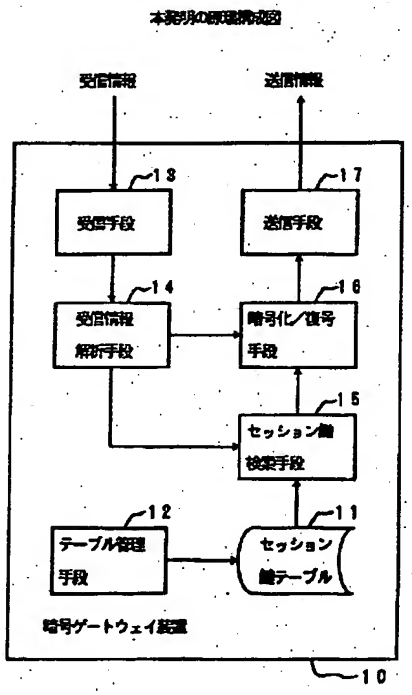
(21)出願番号　特願平5－250850

(22)出願日　平成５年(1993)10月６日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　山口　利和
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　伊東　忠彦

(54)【発明の名称】　暗号ゲートウェイ装置

(57)【要約】
【目的】　本発明は、暗号化／非暗号化の選択及びセッション鍵の選択を端末の組合せ毎又はセッション毎に設定し、既存の端末装置のハードウェア及びアプリケーションプログラムに影響を与えることなく暗号通信を実現する暗号ゲートウェイ装置を提供することを目的とする。
【構成】　本発明の暗号ゲートウェイ装置は、端末の識別情報とセッション鍵の組を保持するセッション鍵テーブル（１１）と、上記組をセッション鍵テーブルに登録する手段（１２）と、受信情報から端末識別情報と通信文を抽出する手段（１４）と、識別情報を検索キーとしてセッション鍵テーブルからセッション鍵を検索する手段（１５）と、識別情報とセッション鍵に応じて通信文を暗号化又は復号する手段（１６）とから成り、セッション鍵の検索の結果該当するセッション鍵が無い場合には通信文を原文のまま送信する構成を特徴とする。



1

【特許請求の範囲】

【請求項１】　受信情報を送信端末から受信し、該受信情報を暗号化又は復号し、該暗号化又は復号された送信情報を受信端末に送信する暗号ゲートウェイ装置において、

送信端末及び受信端末の識別情報と該暗号化又は復号のためのセッション鍵の組を保持するセッション鍵テーブルと、

前記送信端末及び受信端末の識別情報と該セッション鍵を該セッション鍵テーブルに登録するテーブル管理手段と、

前記受信情報から前記送信端末及び受信端末の識別情報と、通信文を抽出する受信情報解析手段と、

該抽出された識別情報を検索キーとして前記セッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と、

前記抽出された識別情報と前記該当するセッション鍵に応じて該通信文を暗号化又は復号して送信情報を作成する暗号化復号手段とから成り、

上記セッション鍵検索手段による検索の結果前記セッション鍵テーブルに該当するセッション鍵が無い場合には前記通信文を原文のまま送信する構成としたことを特徴とする暗号ゲートウェイ装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は暗号ゲートウェイ装置に係り、特に広い地域に分散した事業所等の特定グループ内の端末間で暗号通信を行う場合に、任意の２台の端末が共通のセッション鍵を有することにより暗号通信を行うパケット通信システムにおける暗号ゲートウェイ装置に関する。

【０００２】

【従来の技術】図１０は従来技術による暗号通信システムを説明する図であって、端末ｉ１３０と端末ｊ１４０との間で通信を行う場合、一方の端末ｉ１３０のアプリケーションプログラム１３２（以下、ＡＰと略す）が鍵配送センタ１６０から通信に使用するセッション鍵１６２を取得する。端末ｉ１３０のＡＰｉ３２は、このセッション鍵を通信相手の端末ｊ１４０に送信して、２台の端末で共通のセッション鍵を共有し、これを用いて通信文を暗号化及び復号して暗号通信を行う。

【０００３】図１１は、従来の暗号ゲートウェイ装置１８０を説明する図であって、暗号化／復号を行うための固定セッション鍵１８１と、受信情報を受信するための受信部１８２と、受信情報を解析して通信文を抽出する受信情報解析部１８３と、固定セッション鍵１８１を利用して通信文を暗号化／復号する暗号化／復号部１８４と、暗号化／復号された通信文を送信する送信部１８５とから成る。

【０００４】図１２は、図１１に示す暗号ゲートウェイ

2

装置を利用した暗号通信システムを説明するための図であり、端末21_1、21_2、．．．．、21_nから成るＡグループの端末に暗号ゲートウェイ装置180_1が外付けされ、端末31_1、31_2、．．．．、31_nから成るＢグループの端末に暗号ゲートウェイ装置180_2が外付けされる。暗号ゲートウェイ装置180_1、180_2のセッション鍵は固定であるため、端末21_1と端末31_2の暗号通信と、端末21_nと端末31_2の暗号通信とは共通のセッション鍵で暗号化される。さらに、例えば、端末21_2と端末31_1との通信のように暗号化が不要な通信を行う場合には、暗号ゲートウェイ装置180_1と180_2とを介さない伝送路を用いて通信を行う。

【０００５】

【発明が解決しようとする課題】図１０に示す従来の暗号通信システムでは、暗号通信に先立って、一方の端末上のＡＰが鍵配送センタからセッション鍵を取得し、これを通信相手の端末に送信することが必要であって、端末のＡＰ側の処理が煩雑である。

【０００６】さらに、平文による端末間の通信を暗号通信に対応するよう変更するためには、端末装置のハードウェア又はＡＰを個別に改造する必要があるが、通信システムにおける端末の種類とＡＰは膨大な数に及ぶので、改造の規模及び工数が大きく、従って開発費も大きくなるという問題がある。

【０００７】一方、従来の暗号ゲートウェイ装置を利用する場合には、固定のセッション鍵により画一的に暗号化又は復号がなされるため、通信相手先の端末が暗号通信を行うか、或いは非暗号化通信を行うかに応じて暗号通信のセッション鍵の変更等を行うことができない。

【０００８】本発明は上記の従来の暗号通信システムの問題点に鑑み、暗号通信と非暗号通信の選択と、暗号通信における共有セッション鍵の選択を端末の組合せ毎又はセッション毎に設定し、さらに、既存の端末装置のハードウェア及びＡＰに影響を与えることなく暗号通信を実現する暗号ゲートウェイ装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】図１は本発明の原理構成図である。本発明の暗号ゲートウェイ装置は、受信情報を送信端末から受信し（１３）、該受信情報を暗号化又は復号し、該暗号化又は復号された送信情報を受信端末に送信して（１７）暗号通信を行う装置であって、送信端末及び受信端末の識別情報と暗号化又は復号のためのセッション鍵の組を保持するセッション鍵テーブル（１１）と、送信端末及び受信端末の識別情報とセッション鍵をセッション鍵テーブルに登録するテーブル管理手段（１２）と、受信情報から送信端末及び受信端末の識別情報と、通信文を抽出する受信情報解析手段（１４）と、抽出された識別情報を検索キーとしてセッション鍵

テーブルから該当するセッション鍵を検索するセッション鍵検索手段（１５）と、抽出された識別情報と該当するセッション鍵に応じて通信文を暗号化又は復号して送信情報を作成する暗号化復号手段（１６）とから成り、セッション鍵検索手段による検索の結果セッション鍵テーブルに該当するセッション鍵が無い場合には通信文を原文のまま送信する構成を特徴とする。

【００１０】

【作用】本発明の暗号ゲートウェイ装置は、送信端末と受信端末の組合せ毎又はセッション毎に暗号化用セッション鍵を選定してセッション鍵テーブルを構成し、送信端末から受信した情報により送信元と送信先を識別し、その識別結果をキーとしてセッション鍵テーブルを検索してセッション鍵を得て送信情報の通信文を暗号化又は復号し、セッション鍵が得られない場合には原文のまま送信用通信文として受信端末に送信する。したがって、送信端末から送られた通信文が暗号文と平文のいずれであっても受信することができる。さらに、セッション鍵テーブルを用いることによりセッション鍵を送信端末と受信端末の組合せ毎又はセッション毎に自由に設定できるので、既存の端末に接続する際に、既存の端末ハードウェア、及び、端末のＡＰを改造する必要がない。

【００１１】図２は本発明の暗号ゲートウェイ装置を利用した暗号通信システムの概要を説明する図であり、伝送路４０と、Ａグループの端末２１_{1}、．．．．、２１_{m}と、Ｂグループの端末３１_{1}、．．．．、３１_{n}と、Ｃグループの端末３２_{1}、．．．．、３２_{l}とから成る通信システムにおいて、Ａグループに暗号ゲートウェイ装置Ａを、Ｂグループに暗号ゲートウェイ装置Ｂをさらに設置している。本発明の暗号ゲートウェイ装置により、暗号化と復号が端末の識別情報に応じて判別され、即ち、暗号ゲートウェイ装置が接続されている端末からの送信は暗号化され、暗号ゲートウェイ装置が接続されている端末への送信情報は復号される。さらに、セッション鍵テーブルにセッション鍵が登録されていないセッションに対する通信は、通信文の原文のまま、即ち、平文で通信される。

【００１２】ここで、全ての端末が平文のみを送受信する端末とし、ＡグループとＢグループの間は暗号通信を行ない、ＣグループとＡグループ及びＣグループとＢグループとは非暗号通信を行うことを考える。まず最初に、Ａグループの暗号ゲートウェイ装置Ａ２０のセッション鍵テーブルに、Ａグループの端末２１_{1}、．．．．、２１_{m}を送信元とし、Ｂグループの端末３１_{1}、．．．．、３１_{n}を送信先とするセッションに対するセッション鍵を登録する。本発明の暗号ゲートウェイ装置により、暗号ゲートウェイ装置が接続されている端末からの送信は暗号化を行うので、暗号ゲートウェイ装置Ａ２０は、Ａグループ内の端末からＢグループの端末への送信情報を暗号化して伝送路４０に出力する。次

に、Ｂグループの暗号ゲートウェイ装置Ｂ３０のセッション鍵テーブルにも同様に、Ａグループの端末２１_{1}、．．．．、２１_{m}を送信元とし、Ｂグループの端末３１_{1}、．．．．、３１_{n}を送信先とするセッションに対するセッション鍵を登録する。本発明の暗号ゲートウェイ装置により、暗号ゲートウェイ装置が接続されている端末への送信情報は復号するので、暗号ゲートウェイ装置Ｂ３０は、Ａグループ内の端末からＢグループの端末への送信情報を復号してＢグループ内の端末に出力する。以上により、Ａグループ内の端末からＢグループＢの端末への通信は、各グループ内では平文であって、暗号ゲートウェイ装置を介した伝送路上の通信は暗号文とすることができる。尚、上記と同様にして、Ｂグループの端末３１_{1}、．．．．、３１_{n}を送信元とし、Ａグループの端末２１_{1}、．．．．、２１_{m}を送信先とするセッションに対するセッション鍵をＡグループの暗号ゲートウェイ装置Ａ２０のセッション鍵テーブル及びＢグループの暗号ゲートウェイ装置Ｂ３０のセッション鍵テーブルに登録することにより、Ｂグループ内の端末からＡグループ内の端末への通信を暗号通信化できるようになる。

【００１３】一方、Ａグループの暗号ゲートウェイ装置Ａ２０のセッション鍵テーブル及びＢグループの暗号ゲートウェイ装置Ｂ３０のセッション鍵テーブルには、Ｃグループの端末とにより形成するセッションの登録は行わない。本発明の暗号ゲートウェイ装置により、セッション鍵テーブルにセッション鍵が登録されていないセッションに対しては、平文のまま通信するので、ＡグループとＣグループとの通信及びＢグループとＣグループとの通信は、平文で行われる。

【００１４】次に、端末２１_{1}、２１_{m}、３１_{2}は、暗号文のみを送受信する端末とし、端末２１_{2}、３１_{1}、３１_{n}を平文のみを送受信する端末として、本発明の暗号ゲートウェイ装置を説明する。ここで、暗号ゲートウェイ装置Ａ２０のセッション鍵テーブルには、送信元が端末２１_{2}であって、送信先がＢグループ内の各端末３１_{1}、．．．．、３１_{n}であるセッションと、送信元がＢグループＢの各端末３１_{1}、．．．．、３１_{n}であり、送信先が端末２１_{2}であるセッションに対してセッション鍵を登録する。これにより、端末２１_{2}からの通信文は暗号ゲートウェイ装置Ａ２０により暗号化され、端末２１_{1}、２１_{m}からの通信文は原文、即ち暗号文のまま通過される。したがって、送信元の端末に係わらず、暗号ゲートウェイ装置Ａ２０は、伝送路４０に暗号文を送出する。さらに、暗号ゲートウェイ装置Ｂ３０のセッション鍵テーブルも同様に設定することにより、暗号ゲートウェイ装置Ｂ３０から伝送路４０に送出される通信文は、すべて暗号文とすることができる。したがって、伝送路４０上の通信文はすべて暗号文である。上記の通り、伝送路４０を介してグループＢの端末から暗号ゲートウェイ装置Ａ２０が受信する受信情報は、すべて暗号

5

文である。ここで、暗号ゲートウェイ装置Ａ２０は、セッション鍵テーブルに登録された送信先が端末２１$_2$であるセッションに対する通信文を対応するセッション鍵を用いて復号、即ち平文に変換して端末２１$_2$に送出する。また、送信先が端末２１$_2$以外のセッションに対するセッション鍵はセッション鍵テーブルに登録されていないので、暗号ゲートウェイ装置Ａ２０は、送信先が端末２１$_2$以外の通信文は、原文、即ち暗号文のまま送信先に送出する。

【００１５】

【実施例】以下、コネクション型のプロトコルを利用してネットワークを介して通信を行うＴＣＰ／ＩＰ・ＬＡＮ環境を例として、本発明の一実施例による暗号ゲートウェイ装置の説明を行う。

【００１６】図３は本発明の一実施例の暗号ゲートウェイ装置による暗号通信システムの構成図であり、暗号ゲートウェイ装置１１０と、端末ｉ１３０と、端末ｊ１４０と、ネットワーク１２０から成る。端末ｉ１３０と端末ｊ１４０とが、セッションを確立してネットワーク１２０を介して通信を行う。ここで、端末ｉ１３０と暗号ゲートウェイ装置１１０は、ネットワーク１２０を介して暗号文による通信を行ない、端末ｊ１４０と暗号ゲートウェイ装置１１０は、平文による通信を行うものとする。

【００１７】暗号ゲートウェイ装置１１０は、セッション識別子とセッション鍵の組を保持するセッション鍵テーブル１１１と、セッション鍵テーブル１１１にセッション鍵を登録するテーブル管理部１１２と、情報を受信する受信部１１３と、受信された情報を解析するパケット解析部１１４と、解析された受信情報に含まれるセッション識別子に対応するセッション鍵をセッション鍵テーブル１１１から検索するセッション鍵検索部１１５と、解析された受信情報中の通信文を暗号文又は平文に変換する暗号化／復号部１１６と、暗号化／復号部１１６で変換された通信文又はパケット解析部１１４からの原文のままの通信文を送信する送信部１１７とから成る。

【００１８】図４は、本発明の一実施例によるセッション鍵テーブル１１１を示し、セッションを識別するためのセッション識別子とそのセッション固有のセッション鍵とを保持する。セッション識別子は、送信元及び送信先のネットワーク内でのアドレスを示すための情報であって、送信元のＩＰアドレスとポート番号、及び送信先のＩＰアドレスとポート番号とにより構成される。

【００１９】暗号通信を開始する前に、テーブル管理部１１２が、ＣＲＴ／ＫＢ等の入出力装置、ディスケット、又はネットワーク等を介して入力されたセッション識別子とセッション鍵とをセッション鍵テーブル１１１に登録する。

【００２０】セッション鍵テーブル１１１に登録された

6

セッション識別子を用いて各セッションを一意に識別することができるので、セッション鍵検索部１１５はこのセッション識別子を検索キーとしてセッション鍵を検索することができる。

【００２１】図５は、本発明の一実施例によるＴＣＰ／ＩＰ・ＬＡＮで使用するＯＳＩの参照モデルに準拠したプロトコルであって、データリンクレイヤがＭＡＣ（MediaAccess Control）プロトコル、ネットワークレイヤがＩＰ（Internet Protocol）、トランスポートレイヤがＴＣＰ（Transmit Control Protocol ）で実現され、ＡＰ（アプリケーションプログラム）は、ＴＣＰレイヤ間でセッションを確立する。本発明の一実施例において、ＡＰの通信文（ＡＰデータ）に暗号をかけることにより、ＩＰルータを介したネットワークを使用した通信が可能である。

【００２２】図６は、本発明の一実施例においてＴＣＰ／ＩＰ・ＬＡＮに接続された２台の端末間で通信する際に使用されるパケットのフォーマットを示す図である。パケットは、ＭＡＣヘッダ（ＭＡＣ＿Ｈ）と、ＩＰヘッダ（ＩＰ＿Ｈ）と、ＴＣＰヘッダ（ＴＣＰ＿Ｈ）から構成されるヘッダと、ＡＰデータ及びパケット全体のフレーム・チェック・シーケンス（ＦＣＳ）から構成される。ＡＰデータが暗号化又は復号されて暗号通信が行われる。

【００２３】図７は、本発明の一実施例によるＩＰヘッダのフォーマットを示す図であって、ＩＰヘッダの長さ（単位は４オクテット）を示すＩＨＬ（インターネット・ヘッダ長）と、ＩＰヘッダとＩＰデータ（両者を合わせてＩＰデータグラムという）を加えたオクテット長を示すＴＬ（全長）と、上位層として利用されるプロトコル（本発明の一実施例ではＴＣＰプロトコルであって、値は’６’）を示すＰＲＯＴ（プロトコル）と、送信元ＩＰアドレスを示すＳＲＣ＿ＡＤＲＳ（ソース・アドレス）と、送信先ＩＰアドレスを示すＤＳＴ＿ＡＤＲＳ（デスティネーション・アドレス）とより成る。尚、図中に’－’で示された上記以外のＩＰヘッダの項目については説明を省略するが、ＩＰヘッダの詳細は、「道下、本間：異機種接続とＴＣＰ／ＩＰ絵とき読本、オーム社」に記載されている。

【００２４】パケット解析部１１４は、ＩＨＬにより上位プロトコル（本発明の一実施例ではＴＣＰプロトコル）のヘッダ開始位置を識別する。暗号化／復号部１１６は、ＴＬによりＡＰデータの末尾、即ち暗号化／復号処理の終了位置を識別する。

【００２５】図８は、本発明の一実施例によるＴＣＰヘッダのフォーマットを示す図であって、送信元のポート番号を表すＳＲＣ＿ＰＯＲＴ（ソース・ポート）と、送信先のポート番号を表すＤＳＴ＿ＰＯＲＴ（デスティネーション・ポート）と、ＴＣＰヘッダ長（単位は４オクテット）を示すＤＯ（データ・オフセット）から成る。

7

暗号化／復号部１１６は、ＤＯの値によりＡＰデータの開始位置、即ち暗号化／復号処理の開始位置を識別する。

【００２６】以下では、図３に示すシステムにおいて、受信されたパケットに応じて、端末ｉ１３０から端末ｊ１４０へのＡＰデータは復号し、端末ｊ１４０から端末ｉ１３０へのＡＰデータは暗号化し、端末ｊ１４０が送信元又は送信先に指定された上記以外のＡＰデータは通過（非暗号化）し、その他のパケットは無視するように実現された本発明の暗号ゲートウェイ装置１１０の一実施例を詳細に説明する。

【００２７】図９は、本発明の一実施例による暗号ゲートウェイ装置１１０の暗号化／復号処理を説明するフローチャートである。

【００２８】ステップ１００）受信部１１３は、端末ｉ１３０と端末ｊ１４０との間で通信されるパケットを受信し、受信パケットをパケット解析部１１４に送出する。

【００２９】ステップ１１０）パケット解析部１１４は、受信部１１３より受信パケットを受信し、受信パケットのＭＡＣヘッダからＴＹＰＥ（タイプ）を取り出し、上位プロトコルがＩＰ（値は０ｘ０８００）で無い場合には、受信パケットを送信パケットとして送信部１１７に転送し、ステップ２７０に進む（非暗号通信となる）。

【００３０】ステップ１２０）パケット解析部１１４は、受信パケットのＩＰヘッダからＰＲＯＴ（プロトコル）を取り出し、上位プロトコルがＴＣＰ（値は６）でない場合には、受信パケットを送信パケットとして送信部１１７に転送し、ステップ２７０に進む（非暗号通信となる）。

【００３１】ステップ１３０）パケット解析部１１４は、受信パケットのＩＰヘッダからＴＬ（全長）を取り出し、この値からＩＰデータグラム（ＩＰヘッダ、ＴＣＰヘッダ、及びＡＰデータ）を取得する。

【００３２】ステップ１４０）パケット解析部１１４は、受信パケットのＩＰヘッダからＩＨＬ（インターネット・ヘッダ長）を取り出し、この値に基づいて、ＩＰデータグラムからＩＰヘッダとＩＰデータ（ＴＣＰヘッダとＡＰデータ）とを分離する。

【００３３】ステップ１５０）パケット解析部１１４は、ＴＣＰヘッダからＤＯ（データ・オフセット）を取り出し、この値に基づいて、ＩＰデータからＡＰデータを分離する。

【００３４】ステップ１６０）パケット解析部１１４は、ＩＰヘッダからＳＲＣ＿ＡＤＲＳ（ソース・アドレス）及びＤＳＴ＿ＡＤＲＳ（デスティネーション・アドレス）を取得する。

【００３５】ステップ１７０）パケット解析部１１４は、ＴＣＰヘッダからＳＲＣ＿ＰＯＲＴ（ソース・ポート）及びＤＳＴ＿ＰＯＲＴ（デスティネーション・ポート）を取得する。

8

【００３６】ステップ１８０）セッション鍵検索部１１５は、セッション識別子、即ち、ＳＲＣ＿ＡＤＲＳと、ＤＳＴ＿ＡＤＲＳと、ＳＲＣ＿ＰＯＲＴと、及びＤＳＴ＿ＰＯＲＴをパケット解析部１１４より入力し、入力したセッション識別子をキーとしてセッション鍵テーブル１１１を検索する。

【００３７】ステップ１９０）セッション鍵検索部１１５は、セッション鍵テーブル１１１に上記セッション識別子が登録されていない場合には、パケット解析部１１４の受信パケットを送信パケットとして送信部１１７に転送し、ステップ２７０に進む（非暗号通信となる）。

【００３８】ステップ２００）セッション鍵検索部１１５は、セッション鍵テーブル１１１から検索されたセッション鍵Ｋｓを取得する。

【００３９】ステップ２１０）暗号化／復号部１１４は、パケット解析部１１４の受信パケット、セッション識別子及びＡＰデータと、セッション鍵検索部のセッション鍵Ｋｓと、さらに、暗号ゲートウェイ装置１１０が接続されている端末ｊ１４０のＩＰアドレス（ＩＰ」）を取得する。

【００４０】ステップ２２０）暗号化／復号部１１４は、上記ＩＰ」とセッション識別子中のＳＲＣ＿ＡＤＲＳとを比較して、当該受信パケットの送信方向、即ち、暗号化と復号のいずれであるかを特定する。ＩＰ」とＳＲＣ＿ＡＤＲＳが一致する場合、ステップ２５０に進む。

【００４１】ステップ２３０）暗号化／復号部１１４は、上記ＩＰ」とセッション識別子中のＤＳＴ＿ＡＤＲＳとを比較して、当該パケットの送信方向、即ち、暗号化と復号のいずれであるかを特定する。ＩＰ」とＤＳＴ＿ＡＤＲＳが一致する場合、ステップ２６０に進む。

【００４２】ステップ２４０）当該受信パケットは、暗号ゲートウェイ装置に接続される端末ｊ１４０とは無関係であるため、暗号化／復号部１１４は、当該受信パケットを破棄し、パケット受信に伴う一連動作を終了する。

【００４３】ステップ２５０）暗号化／復号部３６は、ＡＰデータをセッション鍵Ｋｓを用いて暗号化し、ＡＰデータが暗号化された送信パケットを作成し、送信部１１７に転送し（端末ｊ１４０から端末ｉ１３０への暗号化通信）、ステップ２７０に進む。

【００４４】ステップ２６０）暗号化／復号部３６は、ＡＰデータをセッション鍵Ｋｓを用いて復号し、ＡＰデータが復号された送信パケットを作成し（端末ｉ１３０から端末ｊ１４０への復号通信）、送信部１１７に転送する。

【００４５】ステップ２７０）送信部１１７は、送信パケットを端末ｉ１３０又は端末ｊ１４０に送信し、パケ

9

ット受信に伴う一連動作を終了する。

【００４６】尚、上記本発明の一実施例による説明では受信パケット及び送信パケットを各部の間で転送するものとして説明しているが、受信パケット及び送信パケットをバッファに格納し、格納されるアドレスを転送する等、受信パケット及び送信パケットのデータを各部が相互にアクセスできる方法であれば本発明の一実施例に制限されることはない。

【００４７】

【発明の効果】以上説明したように、本発明による暗号ゲートウェイ装置をフロントエンドプロセッサとして端末に接続して、端末間で通信されるパケット等の情報を受信し、情報の送信元と送信先とに応じて、暗号化、復号、又は非暗号化（通過）した情報を送信することにより、既存のＡＰや端末のハードウェアを改造することなく低コストで暗号通信システムを実現することができる。

【００４８】さらに、本発明の暗号ゲートウェイ装置により、各端末間の通信を（暗号文又は平文、及び、同一グループ内又はグループ間を問わず）一切変更すること無く、暗号ゲートウェイ装置を設置したグループ間の通信文をすべて暗号化し、暗号ゲートウェイ装置を設置しないグループとの通信は平文のまま行うことができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の暗号ゲートウェイ装置を利用した暗号通信システムの概要を説明する図である。

【図３】本発明の一実施例によるシステム構成図である。

【図４】本発明の一実施例によるセッション鍵テーブルを説明する図である。

【図５】本発明の一実施例によるＴＣＰ／ＩＰ・ＬＡＮのプロトコルを説明する図である。

【図６】本発明の一実施例によるパケット・フォーマットを説明する図である。

【図７】本発明の一実施例によるＩＰヘッダのフォーマット受信に伴う一連動作を終了する。

【００４６】尚、上記本発明の一実施例による説明では受信パケット及び送信パケットを各部の間で転送するものとして説明しているが、受信パケット及び送信パケットをバッファに格納し、格納されるアドレスを転送する等、受信パケット及び送信パケットのデータを各部が相互にアクセスできる方法であれば本発明の一実施例に制限されることはない。

【００４７】

【発明の効果】以上説明したように、本発明による暗号ゲートウェイ装置をフロントエンドプロセッサとして端末に接続して、端末間で通信されるパケット等の情報を受信し、情報の送信元と送信先とに応じて、暗号化、復号、又は非暗号化（通過）した情報を送信することにより、既存のＡＰや端末のハードウェアを改造することなく低コストで暗号通信システムを実現することができる。

【００４８】さらに、本発明の暗号ゲートウェイ装置により、各端末間の通信を（暗号文又は平文、及び、同一グループ内又はグループ間を問わず）一切変更すること無く、暗号ゲートウェイ装置を設置したグループ間の通信文をすべて暗号化し、暗号ゲートウェイ装置を設置しないグループとの通信は平文のまま行うことができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の暗号ゲートウェイ装置を利用した暗号通信システムの概要を説明する図である。

【図３】本発明の一実施例によるシステム構成図である。

【図４】本発明の一実施例によるセッション鍵テーブルを説明する図である。

【図５】本発明の一実施例によるＴＣＰ／ＩＰ・ＬＡＮのプロトコルを説明する図である。

【図６】本発明の一実施例によるパケット・フォーマットを説明する図である。

【図７】本発明の一実施例によるＩＰヘッダのフォーマットを説明する図である。

【図８】本発明の一実施例によるＴＣＰヘッダのフォーマットを説明する図である。

【図９】本発明の一実施例による暗号化／復号処理のフローチャートである。

【図１０】従来技術を説明する図（その１）である。

【図１１】従来技術を説明する図（その２）である。

【図１２】従来技術による暗号通信システムを説明する図である。

【符号の説明】

１０、２０、３０、１１０　暗号ゲートウェイ装置
１１、１１１　セッション鍵テーブル
１２　テーブル管理手段
１３　受信手段
１４　受信情報解析手段
１５　セッション鍵検索手段
１６　暗号化／復号手段
１７　送信手段
21_1、．．、21_n、31_1、．．、31_n、３
2_1、．．、32_1　端末
４０、４２　伝送路
１１２　テーブル管理部
１１３、１８２　受信部
１１４　パケット解析部
１１５　セッション鍵検索部
１１６、１８４　暗号化／復号部
１１７、１８５　送信部
１２０　ネットワーク
１３０　端末ｉ
１３２、１４２　アプリケーションプログラム
１４０　端末ｊ
１６０　鍵配送センタ
１６２　セッション鍵
１８０、180_1、180_2　暗号ゲートウェイ装置
１８１　固定セッション鍵
１８３　受信情報解析部

【図４】

本発明の一実施例によるセッション鍵テーブル

セッション鍵識別子				セッション鍵
送信元アドレス		送信先アドレス		
IPアドレス	ポート番号	IPアドレス	ポート番号	
IP_S_1	P_S_1	IP_D_1	P_D_1	K_{s1}
IP_S_2	P_S_2	IP_D_2	P_D_2	K_{s2}
⋮	⋮	⋮	⋮	⋮
IP_S_n	P_S_n	IP_D_n	P_D_n	K_{sn}

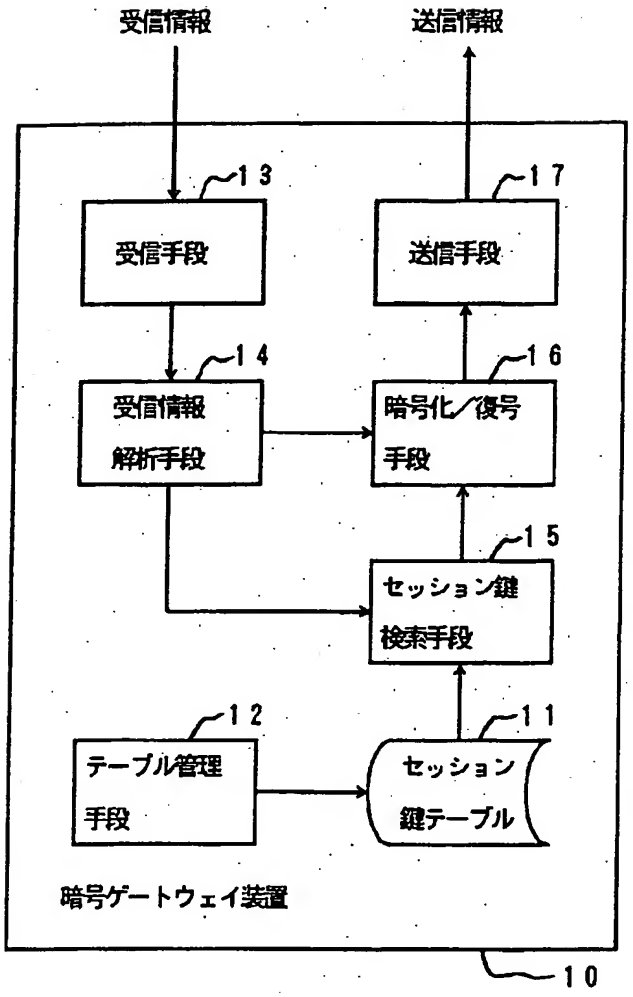
【図５】

本発明の一実施例によるTCP／IP・LANのプロトコル

上位レイヤ	AP
トランスポート	TCP
ネットワーク	IP
データリンク	MAC
物　理	物　理

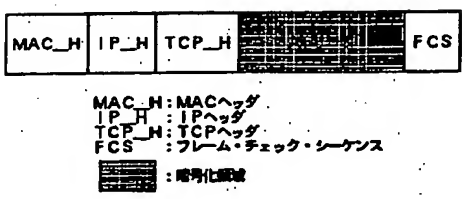
【図１】

本発明の原理構成図



【図６】

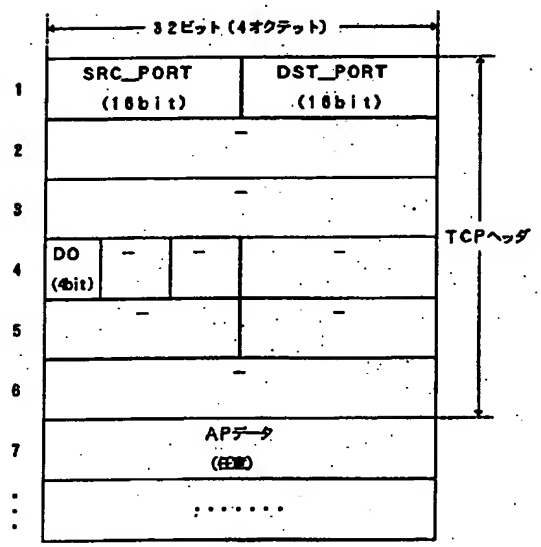
本発明の一実施例によるパケット・フォーマット



MAC_H：MACヘッダ
IP_H　：IPヘッダ
TCP_H：TCPヘッダ
FCS　：フレーム・チェック・シーケンス
：暗号化領域

【図８】

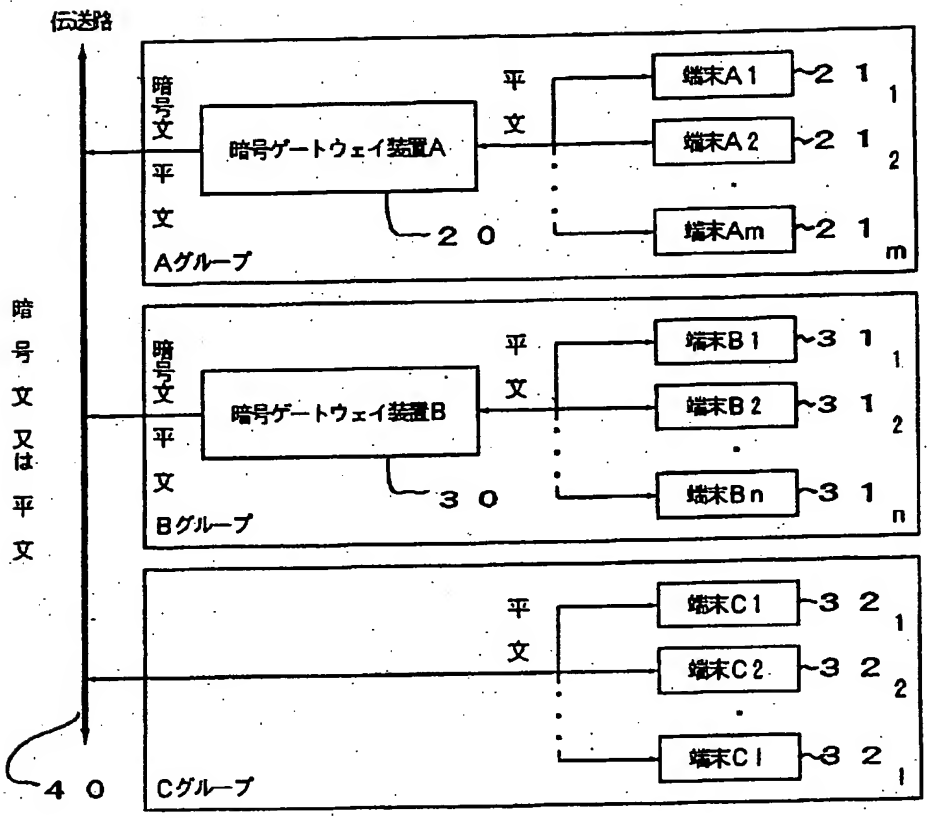
本発明の一実施例によるTCPヘッダのフォーマット



SRC_PORT：ソース・ポート
DST_PORT：デスティネーション・ポート
DO：データ・オフセット

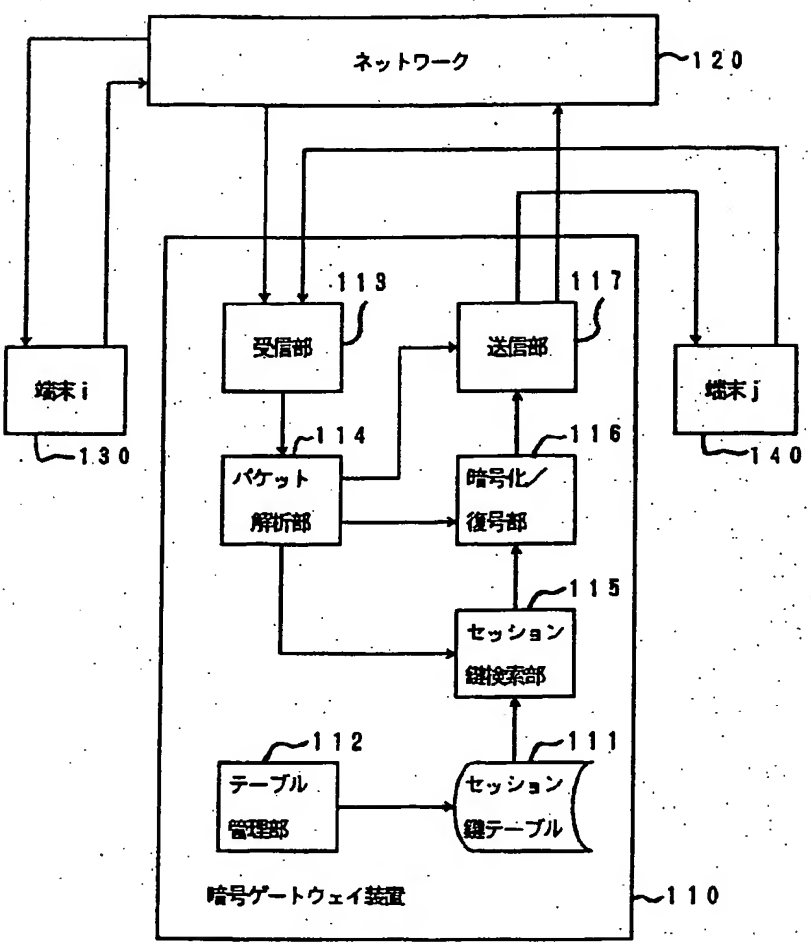
【図２】

本発明の暗号ゲートウェイ装置による
暗号通信システムの概略図



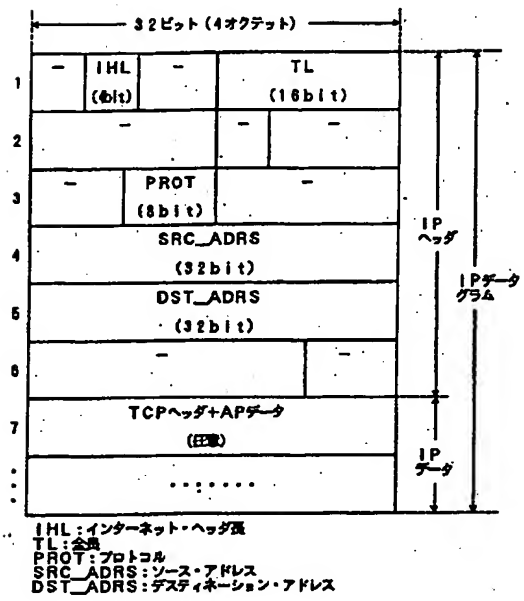
【図３】

本発明の一実施例によるシステム構成図



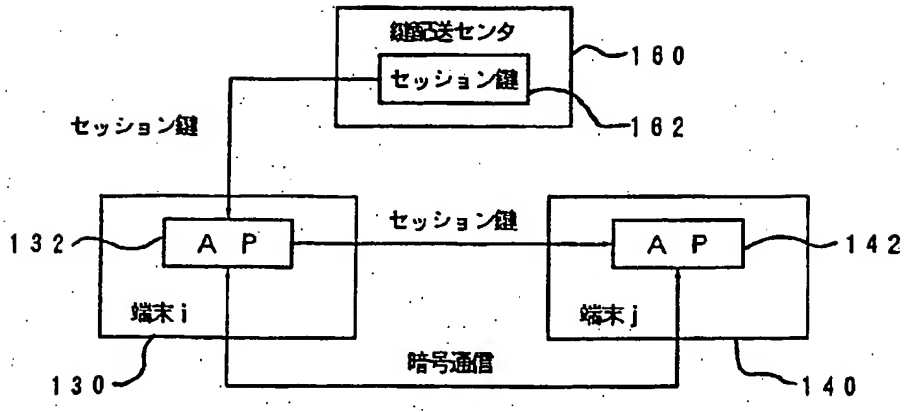
【図7】

本発明の一実施例によるIPヘッダのフォーマット



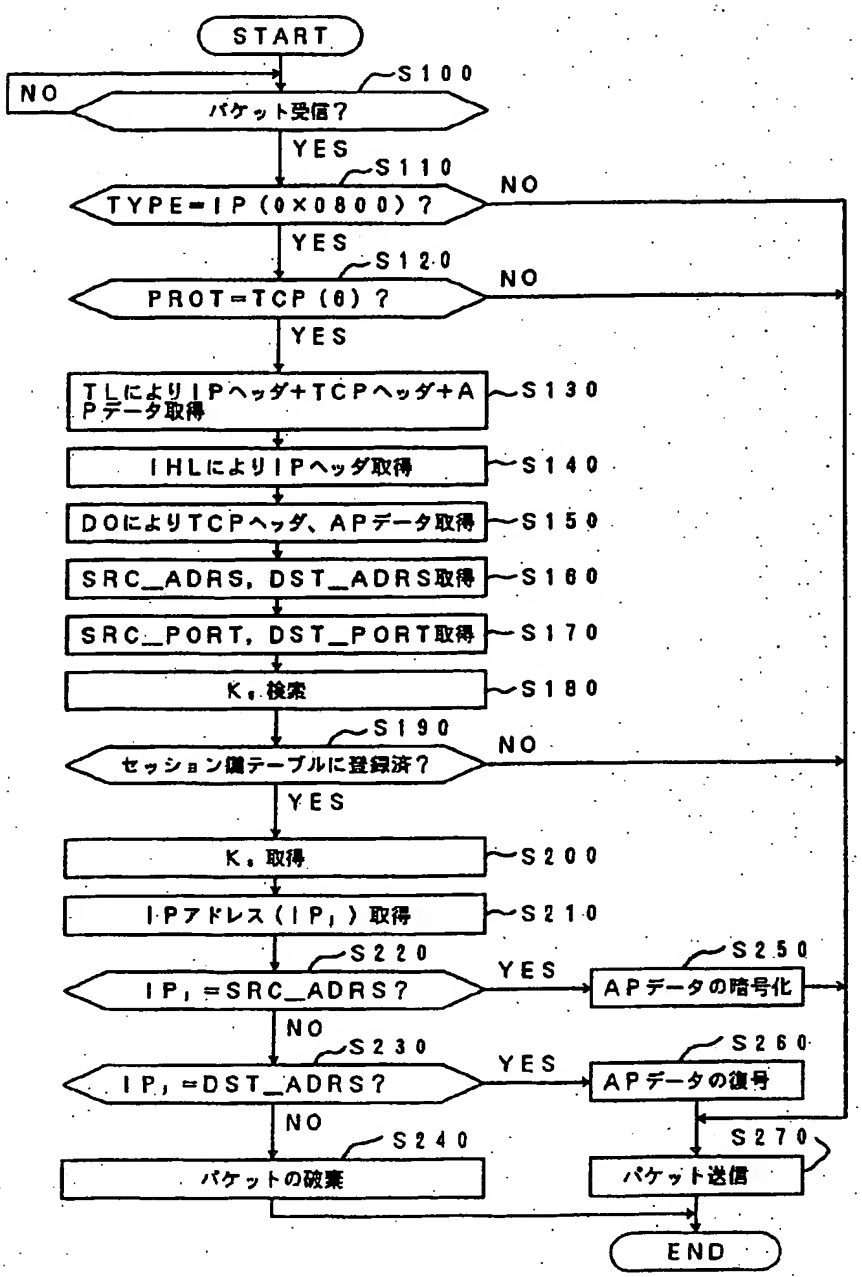
【図10】

従来技術の説明図（その1）



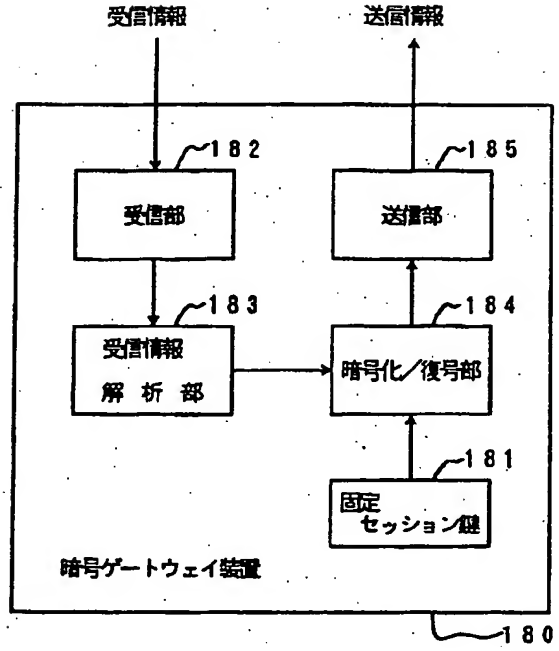
【図9】

本発明の一実施例による暗号化／復号処理のフローチャート



【図１１】

従来技術の説明図（その２）



【図１２】

従来技術による暗号通信システムの説明図